

Approved For Release 2008/05/13 : CIA-RDP89B01354R000100150005-0

**Page Denied**



DEPARTMENT OF STATE

Washington, D.C. 20520

MEMORANDUM

February 1, 1974

TO :   
Chairman  
Computer Security Subcommittee

STAT

FROM : Louis C. Kachulis  
Division of Domestic Operations *JK*  
Office of Security

SUBJECT: Intelligence Community  
Computer Security Policy

FEB 4 5 20 PM '73

We have reviewed the preliminary draft of the proposed policy paper and make the following observations.

It appears to us that the last sentence on page 2 of draft which begins with "Each IC component..." would be more appropriately placed after the first sentence of the second paragraph on page 3, since that paragraph deals specifically with the implementation of the suggested policy.

The final paragraph on page 4 states "Manage or assign responsibility to...". We feel that since responsibility cannot be delegated, this sentence should be changed to read "Manage, or, delegate to subordinate organizations the authority to manage,...".

It seems the entire contents of page 6 and the first half of page 7 are in affect an objective or policy. It is our feeling, therefore, that perhaps the contents of page 6 and the first half of page 7 should be placed after the first paragraph on page 1 under the sub-heading "Purpose".

The last sentence of the first paragraph on page 11 which relates to the use of uncleared maintenance personnel in an emergency, could, it seems, become a

-2-

possible loophole for circumventing the clearance requirements for personnel having access to the computer system. Also, the same sentence states "See paragraph 3, above" it could not be determined to what paragraph it actually references.

Page 12, the second paragraph seems to us to be rather vague in its terminology. Should not the word may be changed to will or should? Also, it would appear that it should be standard procedure, whenever possible, that systems be installed in such a manner that direct access by personnel is limited to a specific system.

The last paragraph on page 12 we feel could be re-written for easier reading as follows: "While the physical and personnel security requirements for the central computer facility area are based upon the overall requirements of the total ADP system, remote terminal area security requirements will be based upon the classification, restrictive categories if any, and the type of material to be accessed through the terminal under system constraints".

The first line on page 16 makes reference to DCID 1/16; it was our understanding that this paper if adopted would replace DCID 1/16 and we question the appropriateness, therefore, of referring to the document. Also on page 16, in order to make the second paragraph read easier, we would suggest the following re-write: When appropriate, provision will be made to permit adjustment of area controls to the level of protection required for the category or type of material actually being handled in the computer, its peripheral devices, and terminals. However, in order to insure the continued reliability and security of the ADP system, and to protect essential hardware or software components of the ADP system, the central computer facility and those components approved for the storage and processing of classified intelligence material may not be downgraded below the level required to protect secure communications equipment.

-3-

On page 17 it appears that some verbage under the "NOTE" was omitted.

Finally, it is suggested that some consideration be given to systems which are already in existance or systems so far progressed on the drawing boards that compliance with the policy, if adopted, would result in exhorbitant and prohibitive costs.